PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-268550
(43)Date of publication of application : 20.09.2002

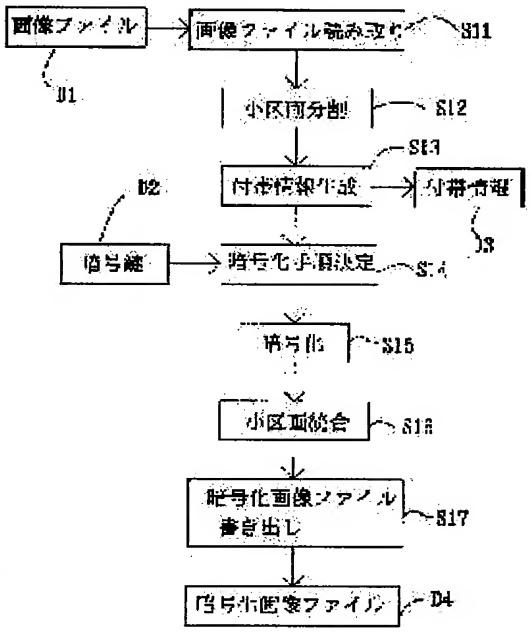
(51)Int.Cl. G09C 1/04
G09C 1/00
H04N 1/44

(21)Application number : 2001-067113
(22)Date of filing : 09.03.2001

(71)Applicant : SEIKO INSTRUMENTS INC
(72)Inventor : ONO SHINSUKE

(54) IMAGE CIPHERING METHOD AND CIPHERING PROGRAM AND RECORDING MEDIUM STORING CIPHERED IMAGE FILE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an image ciphering method and ciphering program by which sketch information can be taken out from ciphered image information even without changing the existing method, device and procedure of image analysis, display, printing and sketch preparation at all.
SOLUTION: This method is provided with a first process S11 of inputting images by reading an image file indicating image information, a second process S12 of performing the optimum small section division of the images from the number of pixels of the image information and a specified parameter and generating accompanying information for the small section division, a third process S13 of replacing the pixels within the small section and performing ciphering for each small section by a prescribed ciphering procedure decided by a specified cipher key and fourth processes S14 and S15 of writing the ciphered image as a ciphered image file indicating the image information.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－268550
（P2002－268550A）
(43)公開日　平成14年９月20日(2002.9.20)

(51)Int.Cl.[7]		識別記号	FI			テーマコード(参考)
Ｇ０９Ｃ	1/04		Ｇ０９Ｃ	1/04		５Ｃ０７５
	1/00	６６０		1/00	６６０Ｄ	５Ｊ１０４
Ｈ０４Ｎ	1/44		Ｈ０４Ｎ	1/44		

審査請求　未請求　請求項の数16　ＯＬ　（全７頁）

(21)出願番号　特願2001－67113(P2001－67113)

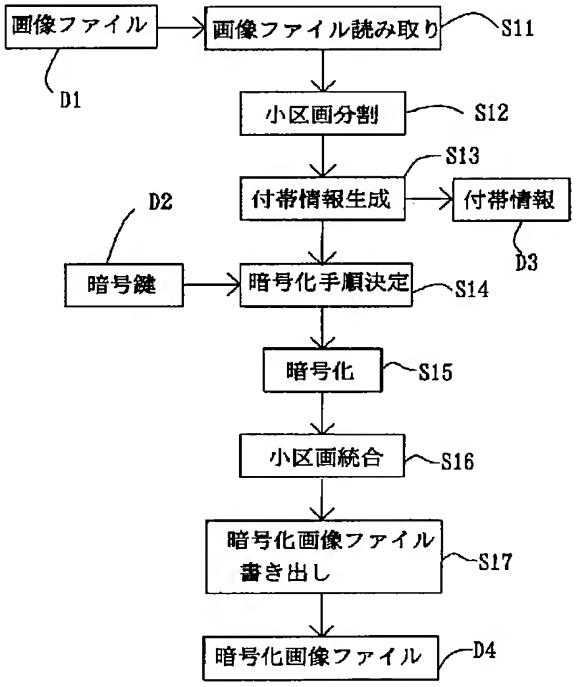
(22)出願日　平成13年３月９日(2001.3.9)

(71)出願人　000002325
セイコーインスツルメンツ株式会社
千葉県千葉市美浜区中瀬１丁目８番地
(72)発明者　大野　伸介
東京都江東区亀戸６丁目31番１号　セイコーアイテック株式会社内
(74)代理人　100096378
弁理士　坂上　正明

Ｆターム(参考)　5C075 CD07 EE03 FF90
5J104 AA15 JA03 NA02 NA12

(54)【発明の名称】　画像の暗号化方法及び暗号化プログラム並びに暗号化画像ファイルを格納した記録媒体

(57)【要約】
【課題】　既存の画像の解析、表示、印刷、略図作成の方法・装置・手順に何ら変更を加えずとも、暗号化画像情報から略図情報を取り出すことを可能な画像の暗号化方法及び暗号化プログラムを提供する。
【解決手段】　画像情報を表す画像ファイルを読み取ることで画像を入力する第１の工程Ｓ１１と、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成する第２の工程Ｓ１２と、指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行う第３の工程Ｓ１３と、暗号化された画像を画像情報を表す暗号化画像ファイルとして書き出す第４の工程Ｓ１４及びＳ１５とを具備する。



1

【特許請求の範囲】

【請求項１】　画像情報を表す画像ファイルを読み取ることで画像を入力する第１の工程と、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成する第２の工程と、指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行う第３の工程と、暗号化された画像を画像情報を表す暗号化画像ファイルとして書き出す第４の工程とを具備することを特徴とする画像の暗号化方法。

【請求項２】　前記暗号鍵及び前記付帯情報に基づいて前記暗号化画像ファイルを復号化する第５の工程をさらに具備することを特徴とする請求項１に記載の画像の暗号化方法。

【請求項３】　前記第３の工程での暗号化を所定の小区画についてのみ行うと共に当該所定の小区画についての第２の付帯情報を生成することを特徴とする請求項１又は２に記載の画像の暗号化方法。

【請求項４】　前記暗号化画像ファイルを復号化する際に前記第２の付帯情報を用いることを特徴とする請求項３に記載の画像の暗号化方法。

【請求項５】　前記暗号化画像ファイルの形式が元の画像ファイルの形式と同一であることを特徴とする請求項１～４の何れかに記載の画像の暗号化方法。

【請求項６】　コンピュータに、画像情報を表す画像ファイルを読み取ることで画像を入力する第１の手順と、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成する第２の手順と、指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行う第３の手順と、暗号化された画像を画像情報を表す暗号化画像ファイルとして書き出す第４の手順とを実行させることを特徴とする画像の暗号化プログラム。

【請求項７】　前記第３の手順では暗号化を所定の小区画についてのみ行うと共に当該所定の小区画についての第２の付帯情報を生成することを特徴とする請求項６に記載の画像の暗号化プログラム。

【請求項８】　前記指定の暗号鍵を与えることにより、前記第１～第４の手順を順次コンピュータに実行させることを特徴とする請求項６又は７に記載の画像の暗号化プログラム。

【請求項９】　画像情報を表す画像ファイルと同一の構造を有し且つ当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成し且つ指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行うことにより生成される暗号化画像情報を表す暗号化画像ファイルを読

2

み取ることで画像を入力する第１の手順と、前記付帯情報に基づいて当該画像の小区画分割を行うと共に前記指定の暗号鍵により決定される前記所定の暗号化手順により前記小区画毎に行う当該小区画内で画素を入れ替えを逆に行って復号化する第２の手順と、復号化された画像を画像情報を表す画像ファイルとして書き出す第３の手順とを、コンピュータに実行させることを特徴とする画像の復号化プログラム。

【請求項１０】　前記指定の暗号鍵及び前記付帯情報を与えることにより前記第１～第３の手順を順次コンピュータに実行させることを特徴とする請求項９に記載の画像の復号化プログラム。

【請求項１１】　前記第３の手順は暗号化を所定の小区画についてのみ行うと共に当該所定の小区画についての第２の付帯情報を生成するものであり、前記第２の手順では、前記第２の付帯情報を用いることを特徴とする請求項９又は１０に記載の画像の復号化プログラム。

【請求項１２】　前記指定の暗号鍵、前記付帯情報及び前記第２の付帯情報を与えることにより前記第１～第３の手順を順次コンピュータに実行させることを特徴とする請求項１１に記載の画像の復号化プログラム。

【請求項１３】　請求項６～１２の何れかのプログラムを記録したことを特徴とするコンピュータに読みとり可能な記録媒体。

【請求項１４】　画像情報を表す画像ファイルと同一の構造を有し、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成し且つ指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行うことにより生成される暗号化画像情報を表す構造を有する暗号化画像ファイルと、前記付帯情報を表す付帯情報データとを記録したことを特徴とするコンピュータに読みとり可能な記録媒体。

【請求項１５】　さらに、前記指定の暗号鍵を与えることにより当該暗号化画像ファイルを復号化する手順をコンピュータに実行させるプログラムを記録したことを特徴とする請求項１４に記載のコンピュータに読みとり可能な記録媒体。

【請求項１６】　前記暗号化画像ファイルは、前記暗号化を所定の小区画についてのみ行われて生成されたものであり、当該所定の小区画についての第２の付帯情報を表すデータをさらに記録したことを特徴とする請求項１４又は１５に記載のコンピュータに読みとり可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、画像を暗号化し、また、暗号化された画像を復号化する画像暗号化方法、画像を暗号化し暗号化された画像を解読する装置、画像

を暗号化し暗号化された画像を解読する手順を記録した記録媒体に関する。

【０００２】

【従来の技術】従来、画像の暗号化方法としては、特開平５－１９９４２４号公報及び特開平６－１２５５５３号公報に開示されているような方法が知られている。このような従来の暗号化方法により暗号化処理した後の暗号画像情報は、画像として表示することは一切できないため、どのような元画像であったかを推測することもできないという問題がある。　また、特開２０００－１０１８５３号に開示されているような方法では、略図を部分的に暗号化しないでおくことができるが、暗号化後の画像情報が一般的な画像形式でなくなるため、特別な方法・装置・手順でなければ暗号化画像から略図を取り出すことはできない。

【０００３】

【発明が解決しようとする課題】上述したように、従来の暗号化処理方法では、暗号化処理した後の暗号画像情報は、一般の画像形式ではないので、復号化しなければ判読できない。従って、例えば、ウェブ上でコンテンツとして暗号化して画像を提供する場合には、サムネイルと呼ばれる縮小画像を添付する必要があるが、何れにしても、サムネイルとバラバラになってしまうと、復号化しない限り画像データの内容が判読できないという問題がある。

【０００４】本発明は、このような事情に鑑み、既存の画像の解析、表示、印刷、略図作成の方法・装置・手順に何ら変更を加えずとも、暗号化画像情報から略図情報を取り出すことを可能な画像の暗号化方法及び暗号化プログラムを提供することを課題とする。

【０００５】

【課題を解決するための手段】前記課題を解決する本発明の第１の態様は、画像情報を表す画像ファイルを読み取ることで画像を入力する第１の工程と、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成する第２の工程と、指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行う第３の工程と、暗号化された画像を画像情報を表す暗号化画像ファイルとして書き出す第４の工程とを具備することを特徴とする画像の暗号化方法にある。

【０００６】本発明の第２の態様は、第１の態様において、前記暗号鍵及び前記付帯情報に基づいて前記暗号化画像ファイルを復号化する第５の工程をさらに具備することを特徴とする画像の暗号化方法にある。

【０００７】本発明の第３の態様は、第１又は２の態様において、前記第３の工程での暗号化を所定の小区画についてのみ行うと共に当該所定の小区画についての第２の付帯情報を生成することを特徴とする画像の暗号化方法にある。

【０００８】本発明の第４の態様は、第３の態様において、前記暗号化画像ファイルを復号化する際に前記第２の付帯情報を用いることを特徴とする画像の暗号化方法にある。

【０００９】本発明の第５の態様は、第１～４の何れかの態様において、前記暗号化画像ファイルの形式が元の画像ファイルの形式と同一であることを特徴とする画像の暗号化方法にある。

【００１０】本発明の第６の態様は、コンピュータに、画像情報を表す画像ファイルを読み取ることで画像を入力する第１の手順と、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成する第２の手順と、指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行う第３の手順と、暗号化された画像を画像情報を表す暗号化画像ファイルとして書き出す第４の手順とを実行させることを特徴とする画像の暗号化プログラムにある。

【００１１】本発明の第７の態様は、第６の態様において、前記第３の手順では暗号化を所定の小区画についてのみ行うと共に当該所定の小区画についての第２の付帯情報を生成することを特徴とする画像の暗号化プログラムにある。

【００１２】本発明の第８の態様は、第６又は７の態様において、前記指定の暗号鍵を与えることにより、前記第１～第４の手順を順次コンピュータに実行させることを特徴とする画像の暗号化プログラムにある。

【００１３】本発明の第９の態様は、画像情報を表す画像ファイルと同一の構造を有し且つ当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成し且つ指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行うことにより生成される暗号化画像情報を表す暗号化画像ファイルを読み取ることで画像を入力する第１の手順と、前記付帯情報に基づいて当該画像の小区画分割を行うと共に前記指定の暗号鍵により決定される前記所定の暗号化手順により前記小区画毎に行う当該小区画内で画素を入れ替えを逆に行って復号化する第２の手順と、復号化された画像を画像情報を表す画像ファイルとして書き出す第３の手順とを、コンピュータに実行させることを特徴とする画像の復号化プログラムにある。

【００１４】本発明の第１０の態様は、第９の態様において、前記指定の暗号鍵及び前記付帯情報を与えることにより前記第１～第３の手順を順次コンピュータに実行させることを特徴とする画像の復号化プログラムにある。

【００１５】本発明の第１１の態様は、第９又は１０の

態様において、前記第３の手順は暗号化を所定の小区画についてのみ行うと共に当該所定の小区画についての第２の付帯情報を生成するものであり、前記第２の手順では、前記第２の付帯情報を用いることを特徴とする画像の復号化プログラムにある。

【００１６】本発明の第１２の態様は、第１１の態様において、前記指定の暗号鍵、前記付帯情報及び前記第２の付帯情報を与えることにより前記第１～第３の手順を順次コンピュータに実行させることを特徴とする画像の復号化プログラムにある。

【００１７】本発明の第１３の態様は、第６～１２の何れかの態様のプログラムを記録したことを特徴とするコンピュータに読みとり可能な記録媒体にある。

【００１８】本発明の第１４の態様は、画像情報を表す画像ファイルと同一の構造を有し、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成し且つ指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行うことにより生成される暗号化画像情報を表す構造を有する暗号化画像ファイルと、前記付帯情報を表す付帯情報データとを記録したことを特徴とするコンピュータに読みとり可能な記録媒体にある。

【００１９】本発明の第１５の態様は、第１４の態様において、さらに、前記指定の暗号鍵を与えることにより当該暗号化画像ファイルを復号化する手順をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータに読みとり可能な記録媒体にある。

【００２０】本発明の第１６の態様は、第１４又は１５の態様において、前記暗号化画像ファイルは、前記暗号化を所定の小区画についてのみ行われて生成されたものであり、当該所定の小区画についての第２の付帯情報を表すデータをさらに記録したことを特徴とするコンピュータに読みとり可能な記録媒体にある。

【００２１】かかる本発明によれば、暗号化した暗号化画像ファイルが、暗号鍵なしでも暗号化前の画像ファイルと同様に一般のアプリケーションで読み込むことができ、元の画像の概略を把握することができる。従って、暗号化した概略画像の著作権を解放することで、画像情報の著作権を持たない者が画像情報を複製保管配布しても、著作者の著作権の侵害に当該しなくなり、画像検索システムを容易に構築できるなどの効果を奏する。

【００２２】

【発明の実施の形態】以下、本発明を一実施形態に基づいて説明する。

【００２３】図１には、一実施形態に係る暗号化方法の手順を示す。必要となるのは、暗号化プログラムと、ＪＰＥＧ、ＧＩＦ、ＢＭＰなどの一般的な形式の画像ファイルＤ１及び暗号鍵Ｄ２であり、暗号化プログラムで画像ファイルＤ１を読み込み、暗号鍵Ｄ２を入力することにより、所定の手順が実行されて暗号化画像ファイルＤ４が出力される。

【００２４】まず、ステップＳ１１で画像ファイルＤ１を読み込むと、画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行う（ステップＳ１２）。ここで、小区画分割はプログラムが自動的に判断するようにしてもよいし、設定できるようにしてもよく、画像の大きさによって、また、暗号化した後に概略がどの程度把握できるか（暗号化の強さ）によって決定すればよく、例えば、８×８、１６×１６、８×１６、６４×６４等を挙げることができる。また、どのような小区分に分割したかについての付帯情報Ｄ３を生成する（ステップＳ１３）。

【００２５】次に、詳細は後述するが、所定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行い（ステップＳ１５）、小区画統合を行う（ステップＳ１６）。暗号化された画像を画像情報を表す暗号化画像ファイルＤ４として書き出す（ステップＳ１７）。ここで、暗号化手順の特長は、小区分内で画素を入れ替えることにより、暗号化を行うことであり、画像情報の形式に影響を与えず、また、暗号化後も画像の全体の雰囲気や色合いなどの概略が把握できるという利点がある。

【００２６】本発明の暗号化プログラムは、図２に示すように、乱数発生アルゴリズム１１及び暗号化手順アルゴリズム１２を具備し、入力された暗号鍵Ｄ２を使用して乱数発生アルゴリズム１１により乱数列１３を得る。また、このようにして得られた乱数列１３を用いて暗号化手順アルゴリズム１２により、暗号化手順１４を得る。

【００２７】ここで、乱数発生アルゴリズム１１は、一般的に知られている、ＤＥＳなどの暗号アルゴリズムや、ＭＤ５、ＳＨＡなどの暗号学のハッシュであり、指定された暗号鍵Ｄ３より、図３に示すような所定の乱数列１３を発生させる。この乱数列１３は暗号鍵Ｄ３により一義的に決定されるが、逆に乱数列１３から暗号鍵Ｄ３を予測することはできないとされている。

【００２８】一方、暗号化手順アルゴリズム１２は、乱数列１３に基づいて所定の画素入れ替え手順を一義的に決定するものである。例えば、一区画区が６４×６４画素の場合の例であるが、乱数列１３の最初から２桁ずつをとって６４より大きいときは６４を引いて６４以内の数字を得、このように得た数字の上から２組ずつを画素入れ替え位置とし、このような画素入れ替えを所定の段数だけ、例えば、６４段繰り返す、というものである。このようにして得られるのが、暗号化手順１４である。

【００２９】このようにして得られた暗号化画像ファイルＤ４は、画像ファイルＤ１と同一の画像形式であり、小区画毎に画素の入れ替えを行っただけなので、暗号鍵Ｄ２なしに、画像の概略を把握することができる。ま

た、暗号化プログラムに画像変換ソフトを組み込んで暗号化と同時に指定の画像形式に変換してもよいことは言うまでもない。

【００３０】図４には、暗号化画像ファイルＤ４の復号化手順を示す。図４に示すように、まず、ステップＳ２１で暗号化画像ファイルＤ４を読み込み、付帯情報Ｄ３に基づいて所定の小区画に分割する（ステップＳ２２）。また、暗号化したときに使用した同一の暗号鍵Ｄ２を用いて復号化手順を決定する（ステップＳ２３）。そして、復号化して（ステップＳ２４）、小区画統合を行い（ステップＳ２５）、画像ファイルＤ５を出力する（ステップＳ２６）。

【００３１】ここで、復号化手順は、例えば、図２に示すような乱数発生アルゴリズム１１及び暗号化手順アルゴリズム１２が決定されていれば、暗号化手順の逆に画素の入れ替えを行う復号化手順を決定することができる。また、画像ファイルＤ５は、通常は暗号化される前の画像ファイルＤ１と同一形式であるが、暗号化の際に画像形式を変換していれば、変換された画像形式のファイルとなる。

【００３２】以上説明した実施形態では、暗号化を分割された小区画の全体に対して小区画毎に行ったが、部分的な小区画のみに対して暗号化を行ってもよい。

【００３３】この手順を図５に示す。この実施形態では、小区画分割を行った（ステップＳ１２）の後、暗号化を行う小区画を決定し、第２の付帯情報Ｄ６を生成する（ステップＳ１３Ａ）。ここで、暗号化する小区画の決定は、プログラムが自動的に判断するようにしてもよいし、設定できるようにしてもよく、第２の付帯情報Ｄ６は、暗号化する小区画を特定できるものであれば、その形式は限定されない。なお、このような暗号化する小区画を決定する第２の付帯情報Ｄ６を生成する場合には、全体を暗号化する際には全体という情報を生成する必要がある。

【００３４】また、このように暗号化された暗号化画像ファイルＤ４を復号化する手順を図６に示す。この場合、付帯情報Ｄ３に基づいて小区画に分割した後、第２の付帯情報Ｄ６により、復号化する小区画を特定し（ステップＳ２２Ａ）、その領域のみ復号化し（ステップＳ２３）する。

【００３５】このように画像の一部分のみを暗号化することにより、暗号化画像ファイルから、概略を把握し易いという効果を奏する。

【００３６】以上説明した暗号化及び復号化の手順の全体を図７に示す。図１～図６と同一作用を示す部分には同一符号を付して説明は省略する。これによれば、画像ファイルＤ１の全体の概略が、暗号化された暗号化画像ファイルＤ４からも把握できることがイメージできる。また、画像ファイルＤ１がカラー画像であれば、小区画毎の画素の入れ替えによる暗号化だから、全体の色合いのイメージも変化しないという利点もある。

【００３７】このような暗号化方法は、既存の暗号アルゴリズムにより、暗号学的な強度が保証されるが、小区画毎に画素を入れ替えるだけであるという画像暗号化アルゴリズムにより、暗号化後も画像の概略を把握できるものである。

【００３８】このような本発明の暗号化方法によれば、画像ファイルをＣＤ－ＲＯＭなどのメディアを介して、又はウェブ上で閲覧、配布し、販売等する場合に、暗号化画像ファイルのみを閲覧させればよく、サムネイルファイルを付帯させる必要はない。また、暗号鍵がなくても暗号化画像ファイルのみから画像の概略が把握できるので、復号化しないと何の画像であるか不明である等の不都合がなくなる。

【００３９】暗号化画像ファイルを閲覧、配布する際に、付帯情報（第２の付帯情報があればそれを含めて）を添付しておき、販売の際に暗号鍵を提示するようにすることにより、安全且つ容易に画像の閲覧、配布及び販売を行うことができる。また、この際、復号化するための暗号化プログラム又は復号化プログラムを同時に配布するようにすればよい。

【００４０】

【発明の効果】以上説明したように、本発明によれば、既存の画像の解析、表示、印刷、略図作成の方法・装置・手順に何ら変更を加えずとも、暗号化画像情報から略図情報を取り出すことを可能な画像の暗号化方法及び暗号化プログラムを提供することができるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る暗号化の手順を示す図である。

【図２】本発明の一実施形態に係る暗号化の手順を説明する図である。

【図３】本発明の一実施形態に係る暗号化の手順を説明する図である。

【図４】本発明の一実施形態に係る復号化の手順を示す図である。

【図５】本発明の他の実施形態に係る暗号化の手順を示す図である。

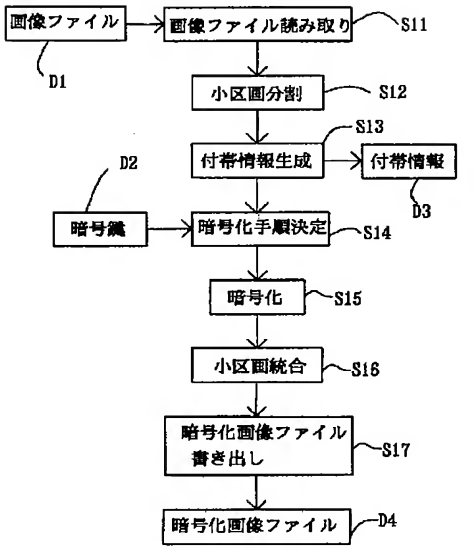
【図６】本発明の他の実施形態に係る復号化の手順を示す図である。

【図７】本発明の暗号化及び復号化の手順を示す図である。

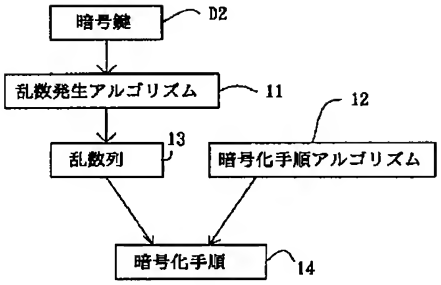
【符号の説明】

Ｄ１、Ｄ５　画像ファイル
Ｄ２　暗号鍵
Ｄ３　付帯情報
Ｄ４　暗号化画像ファイル

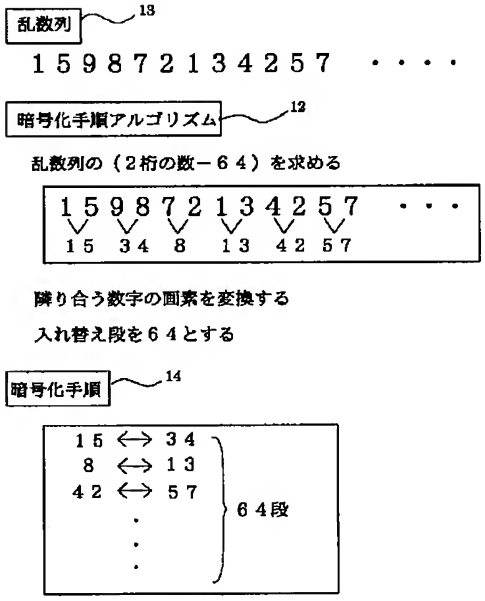
【図１】


画像ファイル
画像ファイル読み取り
S11
D1
小区画分割
S12
付帯情報生成
S13
付帯情報
D3
D2
暗号鍵
暗号化手順決定
S14
暗号化
S15
小区画統合
S16
暗号化画像ファイル
書き出し
S17
暗号化画像ファイル
D4

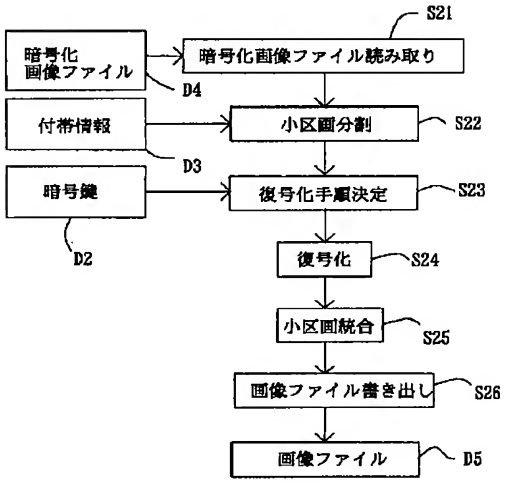
【図２】


暗号鍵
D2
乱数発生アルゴリズム
11
12
乱数列
13
暗号化手順アルゴリズム
暗号化手順
14

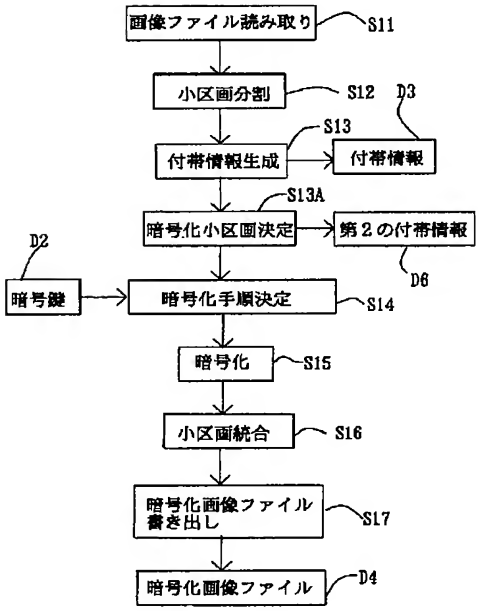
【図３】


乱数列
13
１５９８７２１３４２５７　・・・・
暗号化手順アルゴリズム
12
乱数列の（２桁の数－６４）を求める
１５９８７２１３４２５７　・・・
１５　３４　８　１３　４２　５７
隣り合う数字の画素を変換する
入れ替え段を６４とする
暗号化手順
14
１５ ⟷ ３４
８ ⟷ １３
４２ ⟷ ５７
６４段

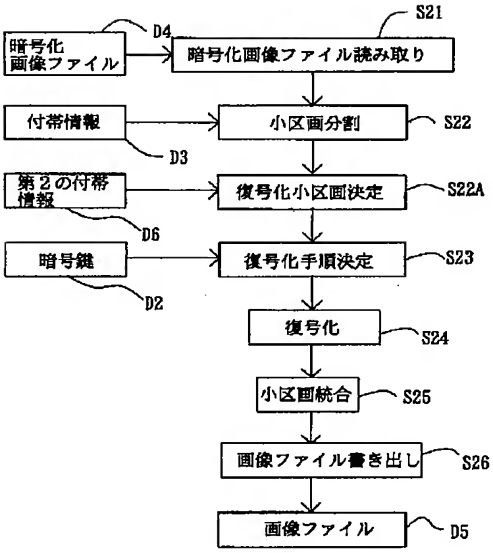
【図４】


S21
暗号化
画像ファイル
暗号化画像ファイル読み取り
D4
付帯情報
小区画分割
S22
D3
暗号鍵
復号化手順決定
S23
D2
復号化
S24
小区画統合
S25
画像ファイル書き出し
S26
画像ファイル
D5

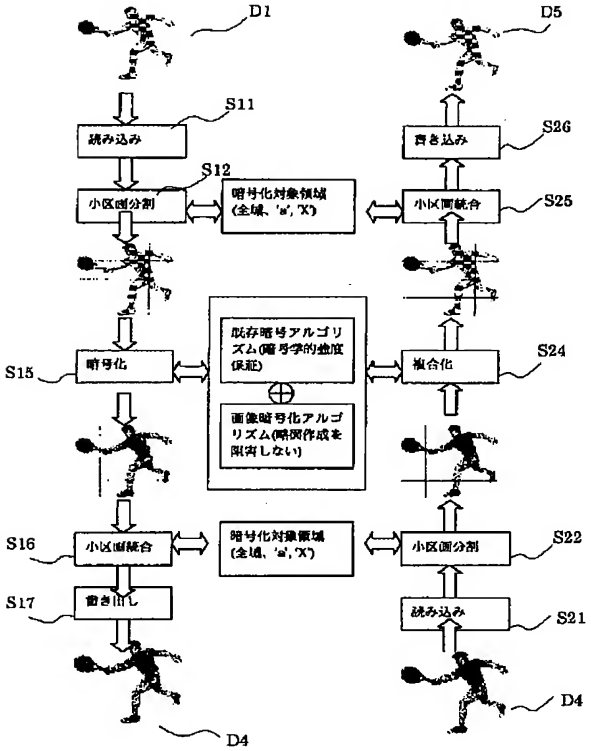
【図５】


画像ファイル読み取り
S11
小区画分割
S12
D3
S13
付帯情報生成
付帯情報
S13A
暗号化小区画決定
第２の付帯情報
D6
D2
暗号鍵
暗号化手順決定
S14
暗号化
S15
小区画統合
S16
暗号化画像ファイル
書き出し
S17
暗号化画像ファイル
D4

【図６】


暗号化
画像ファイル
D4
S21
暗号化画像ファイル読み取り
付帯情報
D3
小区画分割
S22
第２の付帯
情報
D6
復号化小区画決定
S22A
暗号鍵
D2
復号化手順決定
S23
復号化
S24
小区画統合
S25
画像ファイル書き出し
S26
画像ファイル
D5

【図７】


D1
S11
読み込み
S12
小区画分割
暗号化対象領域
(全域、'a'、'X')
S15
暗号化
既存暗号アルゴリズム(暗号学的強度保証)
画像暗号化アルゴリズム(時間作成を限定しない)
S16
小区画統合
暗号化対象領域
(全域、'a'、'X')
S17
書き出し
D4
D5
S26
書き込み
S25
小区画統合
S24
複合化
S22
小区画分割
S21
読み込み
D4